

KEY INFORMATION DISPERSION DEVICE, ARITHMETIC UNIT AND SIGNATURE VERIFICATION DEVICE

Publication number: JP2002091301 (A)

Publication date: 2002-03-27

Inventor(s): SATO HIDENORI +

Applicant(s): NTT DATA CORP +

Classification:

- International: G09C1/00; H04L9/32; G09C1/00; H04L9/32; (IPC1-7): G09C1/00; H04L9/32

- European:

Application number: JP20000284051 20000919

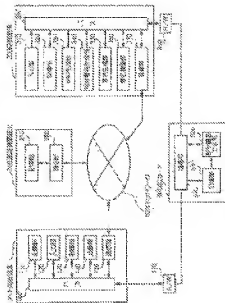
Priority number(s): JP20000284051 20000919

Also published as:

JP4194745 (B2)

Abstract of JP 2002091301 (A)

PROBLEM TO BE SOLVED: To provide a key information dispersion terminal, an IC card and a store terminal capable of improving the secrecy of key information even when a secret key is lost or stolen. **SOLUTION:** The key information dispersion device is provided with a dispersion means for generating partial key information for generating an electronic signature in the case of dividing key information for generating the electronic signature into n (n is a natural number ≥ 2) components and collecting k (k is a natural number of $1 < k \leq n$); divided key information components and a control means for performing either one of control for storing k partial key information components or less out of the partial key information components generated by the dispersion means and control for transmitting k partial key information components or less out of the other partial key information components to a signature verification device by a communication means to an operation unit for generating the electronic signature based on the prescribed program.



Data supplied from the **espacenet** database — Worldwide